Vlastnosti celých čísel

Jan Paseka

Masarykova univerzita Brno

Abstrakt

V této kapitole se budeme zabývat dělitelností a prvočísly.

Abstrakt

V této kapitole se budeme zabývat dělitelností a prvočísly.

Zformulujeme Euklidův algoritmus pro nalezení největšího společného dělitele přirozených čísel.

Abstrakt

V této kapitole se budeme zabývat dělitelností a prvočísly.

Zformulujeme Euklidův algoritmus pro nalezení největšího společného dělitele přirozených čísel.

Ukážeme, že každé netriviální přirozené číslo lze jednoznačným způsobem rozložit na součin prvočísel a že prvočísel je nekonečně mnoho.

Obsah přednášky

- Dělitelnost, dělitel.
- Věta o dělení se zbytkem. Podíl, zbytek.
- Společný dělitel, největší společný dělitel.
- Euklidův algoritmus.
- Bezoutova rovnost.
- Nesoudělnost.

Obsah přednášky

- Dělitelnost, dělitel.
- Věta o dělení se zbytkem. Podíl, zbytek.
- Společný dělitel, největší společný dělitel.
- Euklidův algoritmus.
- Bezoutova rovnost.
- Nesoudělnost.

- Prvočísla.
- Věta o rozkladu na součin prvočísel.
- Prvočísel je nekonečně mnoho.

Dělitelnost I

Pracujeme s množinou

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

všech přirozených čísel

Dělitelnost I

Pracujeme s množinou

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

všech přirozených čísel
a s množinou

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

všech celých čísel.

Dělitelnost I

Pracujeme s množinou

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

všech přirozených čísel
a s množinou

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

všech celých čísel.

Řekneme, že číslo $a \in \mathbb{Z}$ **dělí** číslo $b \in \mathbb{Z}$, jestliže existuje číslo $z \in \mathbb{Z}$ takové, že $b = a \cdot z$.

Dělitelnost II

Pokud číslo $a \in \mathbb{Z}$ **dělí** číslo $b \in \mathbb{Z}$, říkáme, že číslo a je **dělitel** čísla b, a píšeme $a \mid b$.

Dělitelnost II

Pokud číslo $a \in \mathbb{Z}$ **dělí** číslo $b \in \mathbb{Z}$, říkáme, že číslo a je **dělitel** čísla b, a píšeme $a \mid b$.

Speciálně,

- $a \mid 0$ pro každé $a \in \mathbb{Z}$,
- $0 \mid b$ když a jen když $b = 0$.

Věta o dělení celých čísel se zbytkem

Věta. Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Pak existují $q, r \in \mathbb{Z}$ splňující

$$a = b \cdot q + r, \quad 0 \leq r < b.$$

Věta o dělení celých čísel se zbytkem

Věta. Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Pak existují $q, r \in \mathbb{Z}$ splňující

$$a = b \cdot q + r, \quad 0 \le r < b.$$

Přitom čísla q, r jsou určena jednoznačně.

Věta o dělení celých čísel se zbytkem

Věta. Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Pak existují $q, r \in \mathbb{Z}$ splňující

$$a = b \cdot q + r, \quad 0 \leq r < b.$$

Přitom čísla q, r jsou určena jednoznačně.

Poznámka. Číslo q se potom nazývá **podíl** a číslo r **zbytek** po dělení čísla a číslem b. Číslo r označujeme jako $\boxed{a \bmod b.}$

Společný dělitel

Číslo $c \in \mathbb{Z}$ se nazývá **společný dělitel** čísel $a, b \in \mathbb{Z}$, jestliže $c \mid a$ a také $c \mid b$.

Společný dělitel

Číslo $c \in \mathbb{Z}$ se nazývá **společný dělitel** čísel $a, b \in \mathbb{Z}$, jestliže $c \mid a$ a také $c \mid b$.

Číslo $d \in \mathbb{Z}$, které je společným dělitelem čísel a, b a které je přitom největším číslem s touto vlastností, se nazývá **největší společný dělitel** čísel a, b.

Společný dělitel

Číslo $c \in \mathbb{Z}$ se nazývá **společný dělitel** čísel $a, b \in \mathbb{Z}$, jestliže $c \mid a$ a také $c \mid b$.

Číslo $d \in \mathbb{Z}$, které je společným dělitelem čísel a, b a které je přitom největším číslem s touto vlastností, se nazývá **největší společný dělitel** čísel a, b.
Je-li $a \neq 0$ nebo $b \neq 0$, pak tento největší společný dělitel d čísel a, b existuje, přitom $d \in \mathbb{N}$, a značí se (a, b).

Společný dělitel

Číslo $c \in \mathbb{Z}$ se nazývá **společný dělitel** čísel $a, b \in \mathbb{Z}$, jestliže $c \mid a$ a také $c \mid b$.

Číslo $d \in \mathbb{Z}$, které je společným dělitelem čísel a, b a které je přitom největším číslem s touto vlastností, se nazývá **největší společný dělitel** čísel a, b.
Je-li $a \neq 0$ nebo $b \neq 0$, pak tento největší společný dělitel d čísel a, b existuje, přitom $d \in \mathbb{N}$, a značí se (a, b).
Je-li $a = b = 0$, pak největší společný dělitel čísel a, b podle dané definice neexistuje.

Euklidův algoritmus

Metoda pro nalezení největšího společného dělitele (a, b) dvou čísel $a, b \in \mathbb{N}$.

Euklidův algoritmus

Metoda pro nalezení největšího společného dělitele (a, b) dvou čísel $a, b \in \mathbb{N}$.

Provádí se postupně následující dělení se zbytkem.

Euklidův algoritmus

Metoda pro nalezení největšího společného dělitele (a, b) dvou čísel $a, b \in \mathbb{N}$.

Provádí se postupně následující dělení se zbytkem.

$$\begin{array}{lll} \text{while} & a \neq 0 & \text{do} \\ & r \longleftarrow & a \bmod b \\ & a \longleftarrow & b \\ & b \longleftarrow & r \\ \text{return} & & \end{array}$$

Příklad na Euklidův algoritmus

Nalezněte $(143, 110)$.

Příklad na Euklidův algoritmus

Nalezněte $(143, 110)$.

$$143 \;=\; 1 \;\times\; 110 \;+\; 33$$

Příklad na Euklidův algoritmus

Nalezněte $(143, 110)$.

$$\begin{aligned} 143 &= 1 \times 110 + 33 \\ 110 &= 3 \times 33 + 11 \end{aligned}$$

Příklad na Euklidův algoritmus

Nalezněte $(143, 110)$.

$$\begin{aligned} 143 &= 1 \times 110 + 33 \\ 110 &= 3 \times 33 + 11 \\ 33 &= 3 \times 11 + 0 \end{aligned}$$

Příklad na Euklidův algoritmus

Nalezněte $(143, 110)$.

$$\begin{array}{rcccccccc} 143 & = & 1 & \times & 110 & + & 33 \\ 110 & = & 3 & \times & 33 & + & 11 \\ 33 & = & 3 & \times & 11 & + & 0 \end{array}$$

Výsledek: $(143, 110) = 11$.

Matematický popis Euklidova algoritm

Postupně se tedy hledají čísla $q_0, q_1, \ldots, q_n$, $q_{n+1} \in \mathbb{N} \cup \{0\}$ a $r_0, r_1, \ldots, r_n \in \mathbb{N}$ taková, že platí:

Matematický popis Euklidova algoritm

Postupně se tedy hledají čísla $q_0, q_1, \ldots, q_n$, $q_{n+1} \in \mathbb{N} \cup \{0\}$ a $r_0, r_1, \ldots, r_n \in \mathbb{N}$ taková, že platí:

$$
\begin{aligned}
a &= b \cdot q_0 + r_0, \quad 0 \le r_0 < b, \\
b &= r_0 \cdot q_1 + r_1, \quad 0 \le r_1 < r_0, \\
r_0 &= r_1 \cdot q_2 + r_2, \quad 0 \le r_2 < r_1, \\
r_1 &= r_2 \cdot q_3 + r_3, \quad 0 \le r_3 < r_2, \\
&\ldots \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n, \quad 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n \cdot q_{n+1} + 0.
\end{aligned}
$$

Ukončení a korektnost Eukl. algoritmu

Poslední dělení $r_{n-1} = r_n \cdot q_{n+1} + 0$ je tvaru $r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$, kde $r_{n+1} = 0$.

Ukončení a korektnost Eukl. algoritmu

Poslední dělení $r_{n-1} = r_n \cdot q_{n+1} + 0$ je tvaru $r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$, kde $r_{n+1} = 0$.

Poněvadž $b > r_0 > r_1 > r_2 > \ldots$, musí tato posloupnost dělení skončit tímto způsobem.

Ukončení a korektnost Eukl. algoritmu

Poslední dělení $r_{n-1} = r_n \cdot q_{n+1} + 0$ je tvaru $r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$, kde $r_{n+1} = 0$.

Poněvadž $b > r_0 > r_1 > r_2 > \ldots$, musí tato posloupnost dělení skončit tímto způsobem.

- Pro $r_0 = 0$, tj. $b \mid a$ a tedy $(a, b) = b$, položme $n = -1$ a označme ještě $r_{-1} = b$.

Ukončení a korektnost Eukl. algoritm

Poslední dělení $r_{n-1} = r_n \cdot q_{n+1} + 0$ je tvaru $r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$, kde $r_{n+1} = 0$.

Poněvadž $b > r_0 > r_1 > r_2 > \ldots$, musí tato posloupnost dělení skončit tímto způsobem.

- Pro $r_0 = 0$, tj. $b \mid a$ a tedy $(a, b) = b$, položme $n = -1$ a označme ještě $r_{-1} = b$.
- Pro $r_0 > 0$ existuje $n \in \mathbb{N} \cup \{0\}$ takové, že $r_{n+1} = 0$.

Ukončení a korektnost Eukl. algoritmu

Poslední dělení $r_{n-1} = r_n \cdot q_{n+1} + 0$ je tvaru $r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$, kde $r_{n+1} = 0$.

Poněvadž $b > r_0 > r_1 > r_2 > \dots$, musí tato posloupnost dělení skončit tímto způsobem.

- Pro $r_0 = 0$, tj. $b \mid a$ a tedy $(a, b) = b$, položme $n = -1$ a označme ještě $r_{-1} = b$.
- Pro $r_0 > 0$ existuje $n \in \mathbb{N} \cup \{0\}$ takové, že $r_{n+1} = 0$.

Věta. Nechť $a, b \in \mathbb{N}$. Pak $(a, b) = r_n$.

Bezoutova rovnost

Věta. Pro libovolná $a, b \in \mathbb{Z}$ taková, že $a \neq 0$ nebo $b \neq 0$, existují $u, v \in \mathbb{Z}$ taková, že $(a, b) = a \cdot u + b \cdot v$.

Bezoutova rovnost

Věta. Pro libovolná $a, b \in \mathbb{Z}$ taková, že $a \neq 0$ nebo $b \neq 0$, existují $u, v \in \mathbb{Z}$ taková, že $(a, b) = a{\cdot}u + b{\cdot}v$.

Důsledek. Nechť $a, b \in \mathbb{Z}$, $a \neq 0$ nebo $b \neq 0$. Pak číslo $d \in \mathbb{N}$ je největším společným dělitelem čísel a, b, právě když $d \mid a$, $d \mid b$ a je splněna podmínka, že pro každé číslo $e \in \mathbb{N}$ s vlastností, že $e \mid a$, $e \mid b$, platí $e \mid d$.

Nesoudělnost

Řekneme, že čísla $a, b \in \mathbb{Z}$ jsou **nesoudělná**, jestliže $(a, b) = 1$.

Nesoudělnost

Řekneme, že čísla $a, b \in \mathbb{Z}$ jsou **nesoudělná**, jestliže $(a, b) = 1$.

Důsledek. Jestliže pro čísla $a, b, c \in \mathbb{Z}$ platí $a \mid b \cdot c$ a současně $(a, b) = 1$, pak odtud plyne $a \mid c$.

Prvočísla

Přirozené číslo $p \geq 2$ se nazývá **prvočíslo**, jestliže přirozenými čísly, která jsou jeho děliteli, jsou pouze čísla 1 a p.

Prvočísla

Přirozené číslo $p \geq 2$ se nazývá **prvočíslo**, jestliže přirozenými čísly, která jsou jeho děliteli, jsou pouze čísla 1 a p.

Věta. Pro každé přirozené číslo $a \geq 2$ platí, že buďto a je prvočíslo, anebo a je možno rozložit na součin prvočísel, přičemž tento rozklad je jediný až na pořadí činitelů.

Prvočísla

Přirozené číslo $p \geq 2$ se nazývá **prvočíslo**, jestliže přirozenými čísly, která jsou jeho děliteli, jsou pouze čísla 1 a p.

Věta. Pro každé přirozené číslo $a \geq 2$ platí, že buďto a je prvočíslo, anebo a je možno rozložit na součin prvočísel, přičemž tento rozklad je jediný až na pořadí činitelů.

Důsledek. Existuje nekonečně mnoho prvočísel.